LUISS

SCHEDA TECNICA A

Scheda Tecnica A allegata al D.R. n. ..... del .....

Titolo del progetto di ricerca	Strategie di sicurezza per l'Intelligenza Artificiale: metriche, processi e pratiche organizzative.	
Argomenti di Ricerca e Innovazione sulla Cybersicurezza (Aree approfondite nel progetto di ricerca)	**Argomento 1**	Argomento#6.2.1: lo studio e il miglioramento continuo dei quadri procedurali per la valutazione del rischio, al fine di facilitare l'identificazione, l'analisi e la quantificazione del rischio rendendo quindi più efficace il relativo piano di trattamento (e l'accettazione del rischio ove ragionevole). In particolare, rientrano in questo argomento di R&I i modelli per la valutazione d'impatto.
	Argomento 2	Argomento#6.3.1: l'innovazione nella standardizzazione dei processi aziendali per la cybersicurezza, sfruttando, ad esempio, i Capability Maturity Model (CMM) e i modelli di sicurezza zero trust.
	Argomento 3	Argomento#6.1.1: la ricerca sull'economia dell'ecosistema della cybersicurezza e, in particolare, delle catene di approvvigionamento (supply chain)
OBIETTIVI DEL PROGETTO E CAPACITÀ DI REALIZZAZIONE		

obiettivi del progetto	La sicurezza dell'Intelligenza Artificiale rappresenta una sfida cruciale per le organizzazioni, che devono bilanciare la protezione dei sistemi con la sostenibilità economica degli investimenti e la necessità di adottare pratiche standardizzate. Questo progetto di ricerca si propone di sviluppare un framework integrato che aiuti le imprese e i policy maker a gestire i rischi legati all'IA attraverso strumenti di valutazione economica, modelli di maturità della sicurezza e incentivi di mercato. Un primo obiettivo è l'applicazione del Return on Security Investment (ROSI) come strumento di supporto alle decisioni strategiche, affinché i manager possano allocare risorse per la protezione dell'IA in modo proporzionato al rischio e coerente con le esigenze di governance e regolamentazione. L'analisi dei rischi specifici dell'IA generativa permetterà di sviluppare metriche che guidino l'ottimizzazione degli investimenti, assicurando un equilibrio tra costi, benefici e livello di sicurezza raggiunto. Parallelamente, il progetto esplora il ruolo del Capability Maturity Model (CMM) come leva per promuovere la sicurezza nei mercati dell'IA. I modelli di maturità forniscono un quadro strutturato per migliorare progressivamente le capacità di protezione, incentivando sia le organizzazioni che offrono servizi IA-based sia i policy maker ad adottare standard condivisi. A partire da questa prospettiva, il progetto propone lo sviluppo di un AI Security Index, un indicatore che consenta di misurare il livello di sicurezza delle imprese lungo la filiera dell'IA, incentivando il miglioramento continuo delle pratiche di cybersecurity. Infine, il progetto integra una riflessione sull'economia della cybersicurezza e sulla sicurezza lungo le catene di approvvigionamento dell'IA. Considerare la protezione dei sistemi IA non solo a livello organizzativo, ma come un obiettivo comune dell'intero ecosistema, consente di evidenziare il ruolo degli investimenti in sicurezza nella

	resilienza delle supply chain digitali. La combinazione tra ROSI, AI Security Index e governance della sicurezza aiuterà a definire strategie più efficaci per proteggere le infrastrutture critiche dell'IA e promuovere una maggiore collaborazione tra imprese, fornitori e istituzioni. Attraverso questo approccio integrato, il progetto mira a fornire strumenti pratici e teorici per una gestione più efficace della sicurezza dell'IA, favorendo una convergenza tra valutazione economica, governance della sicurezza e standardizzazione nei mercati.
Pertinenza del progetto agli argomenti dell'Agenda	Il progetto si allinea con tre tematiche chiave dell'Agenda di ricerca, offrendo un contributo teorico e applicativo su valutazione del rischio, standardizzazione della sicurezza e gestione delle supply chain digitali. In primo luogo, il progetto risponde all'Argomento 6.2.1, che riguarda lo studio e il miglioramento continuo dei quadri procedurali per la valutazione del rischio. L'integrazione del ROSI permette di sviluppare metriche per quantificare i rischi specifici dell'IA generativa e valutare l'impatto economico delle strategie di sicurezza. Questo approccio contribuirà a una più efficace identificazione, analisi e mitigazione del rischio, rendendo il piano di trattamento più strutturato e sostenibile. In secondo luogo, il progetto è coerente con l'Argomento 6.3.1, relativo all'innovazione nella standardizzazione dei processi aziendali per la cybersicurezza. L'uso del CMM fornisce un modello per misurare e incentivare il miglioramento progressivo della sicurezza dell'IA, facilitando l'adozione di pratiche condivise. Inoltre, lo sviluppo dell'AI Security Index rappresenta un contributo innovativo, poiché permette di valutare la maturità della sicurezza IA nelle organizzazioni e di creare incentivi per il miglioramento continuo delle pratiche di protezione. Infine, il progetto affronta l'Argomento 6.1.1, che riguarda la ricerca sull'economia della cybersicurezza e sulla sicurezza lungo la supply chain. L'AI Security Index può

	diventare uno strumento strategico per misurare e incentivare la sicurezza lungo l'intera catena del valore dell'IA, creando un meccanismo di mercato che spinga le imprese ad adottare livelli di protezione più elevati. L'integrazione con il ROSI consente di allineare le scelte di investimento alla necessità di una sicurezza distribuita, contribuendo alla resilienza dell'ecosistema IA nel suo complesso.
Modalità di realizzazione del progetto, anche in termini di fattori abilitanti a disposizione	Il progetto di dottorato si sviluppa in quattro anni, integrando ricerca teorica, sviluppo di modelli e validazione empirica attraverso la collaborazione con imprese e istituzioni nel settore della sicurezza e dell'intelligenza artificiale. Nel primo anno, il candidato acquisirà preparazione metodologica con corsi avanzati in scienze sociali, analisi qualitativa e quantitativa, e cybersecurity, insieme a tematiche su management, sistemi informativi e governance digitale. Questo garantirà una solida base interdisciplinare per affrontare le sfide della sicurezza dell'IA e della gestione del rischio digitale. Nel secondo anno, si svilupperà un framework di valutazione economica della sicurezza dell'IA, integrando il ROSI per le decisioni sugli investimenti e il CMM per migliorare la sicurezza nei mercati IA-based. Si esploreranno anche tecniche di simulazione, come il metodo Monte Carlo, per affinare le metriche di valutazione del rischio. Saranno avviate interazioni con imprese e stakeholder, testando il framework tramite studi di caso. La collaborazione con il Competence Center Cyber 4.0 e la cattedra Fastweb+Vodafone faciliterà l'accesso all'ecosistema industriale avanzato. Nel terzo anno, il framework sarà testato in contesti organizzativi con IA generativa, con validazione dell'AI Security Index, volto a misurare la sicurezza delle imprese lungo la filiera dell'IA. La collaborazione con il centro di

	ricerca AI4Society garantirà un ambiente multidisciplinare. Nel quarto anno, il progetto si concentrerà sulla finalizzazione dell'analisi integrando i feedback ricevuti nel confronto con network accademici nazionali e internazionali attraverso il Dottorato in Cybersecurity, la comunità ITASEC, la comunità AIS (Association for Information Systems), la comunità di Design Science Research (DESRIST), il network ERCIS (European Research Center for Information Systems), la comunità European Safety and Reliability (ESREL) e la Society for Risk Analysis Europe (SRA-E).	
ELEMENTI DEL PROGETTO RELATIVI ALLE TEMATICHE PRIORITARIE		
Contributo distintivo del progetto in relazione agli argomenti prioritari	**Argomento 1**	Argomento#6.2.1: lo studio e il miglioramento continuo dei quadri procedurali per la valutazione del rischio, al fine di facilitare l'identificazione, l'analisi e la quantificazione del rischio rendendo quindi più efficace il relativo piano di trattamento (e l'accettazione del rischio ove ragionevole). In particolare, rientrano in questo argomento di R&I i modelli per la valutazione d'impatto.
	Argomento 2	Argomento#6.3.1: l'innovazione nella standardizzazione dei processi aziendali per la cybersicurezza, sfruttando, ad esempio, i Capability Maturity Model (CMM) e i modelli di sicurezza zero trust.
	Argomento 3	Argomento#6.1.1: la ricerca sull'economia dell'ecosistema della

		cybersicurezza e, in particolare, delle catene di approvvigionamento (supply chain)
	Il progetto di ricerca contribuisce in modo innovativo alla gestione dei rischi legati all'Intelligenza Artificiale (IA) e alla sicurezza nei sistemi IA, con particolare attenzione alla standardizzazione dei processi aziendali per la cybersicurezza, come previsto dall'Agenda di Ricerca e Innovazione per la Cybersicurezza. Il framework sviluppato aiuterà le organizzazioni nell'allocazione degli investimenti per la sicurezza dell'IA, combinando valutazione economica e sicurezza, e sarà applicabile a livello aziendale e per i policy maker. L'approccio si basa sul Return on Security Investment (ROSI) e sull'AI Security Index, strumenti che permettono di definire gli interventi prioritari e di standardizzare le linee guida per la sicurezza dell'IA. Questo consentirà alle pubbliche amministrazioni e agli enti regolatori di indirizzare gli investimenti in cybersecurity in modo mirato, con uno score quantitativo che collega il ritorno sugli investimenti alla protezione dai rischi legati all'IA. Inoltre, il framework faciliterà la raccolta sistematica e standardizzata dei dati sulla sicurezza delle organizzazioni, migliorando la capacità di monitorare e rafforzare continuamente la sicurezza nel tempo. Questo approccio garantirà una maggiore uniformità nei processi di valutazione e monitoraggio della sicurezza, migliorando la gestione del rischio a livello aziendale ed ecosistemico e stimolando una maggiore collaborazione tra pubblico e privato. Il progetto affronta anche la sfida della governance della sicurezza nell'adozione e sviluppo delle tecnologie IA, combinando ROSI e Capability Maturity Model (CMM) per supportare la pianificazione strategica degli investimenti in sicurezza. Il framework proposto si	

	configura come uno strumento chiave per rafforzare la resilienza dell'ecosistema digitale, promuovendo la standardizzazione e la diffusione delle migliori pratiche in cybersecurity, con un impatto significativo sulla crescita delle applicazioni IA nel mercato.
COLLABORAZIONI CON ALTRI SOGGETTI PUBBLICI E PRIVATI	
Motivazione ed evidenze del coinvolgimento nel progetto di ricerca di imprese, enti e laboratori di ricerca pubblici o privati riconducibili a realtà italiane e/o europee, organismi internazionali	Il progetto beneficia di un ampio network di collaborazioni con enti e imprese nazionali e internazionali, garantendo al dottorando accesso a risorse fondamentali e un impatto significativo sulla sicurezza dell'IA. In particolare, si inserisce nel contesto del progetto PRIN Data4Innovation, che ha esplorato la data governance in ambienti distribuiti, ponendo le basi per affrontare le sfide legate alla sicurezza dei dati, tema cruciale nell'ambito della cybersicurezza. La cattedra Fastweb+Vodafone e le collaborazioni del centro AI4Society sui temi dell'AI e della data governance con la rete di Confindustria, offre l'opportunità di raccogliere dati sulla cybersecurity, testando il framework di valutazione della sicurezza. La connessione diretta tra ricerca e mercato migliorerà la validità applicativa dei risultati. Queste collaborazioni garantiranno che il framework proposto sia allineato con le esigenze di ricerca e le pratiche di sicurezza internazionali.
Svolgimento di un periodo di studio all'estero nei Paesi dell'Unione Europea contestualizzato al progetto di ricerca	Il progetto di dottorato prevede un periodo di studio all'estero che si svolgerà presso una delle università o centri di ricerca membri dell'Alleanza europea ENGAGE.EU, di cui Luiss è partner. La scelta dell'istituzione ospitante dipenderà dalle opportunità che si apriranno all'interno del network, che include rinomate università europee: Tilburg, Mannheim, Sofia (University of National and World Economy), Tolosa Capitole, Vienna (WU), Hanken School of Economics (Helsinki/Vaasa),

	Ramon Llull (Barcellona) e Norwegian School of Economics (NHH) di Bergen. Durante questo periodo, il dottorando avrà l'opportunità di collaborare con ricercatori impegnati sui temi della digitalizzazione. In particolare, la possibilità di partecipare a iniziative all'interno dell'Industry-Academia Network of the Cybersecurity Skills Academy, che rientra tra le iniziative promosse da ENGAGE.EU, consentirà al dottorando di sviluppare competenze applicate nella gestione della sicurezza delle tecnologie emergenti, integrando la teoria con l'esperienza pratica sul campo. Inoltre, il dottorando potrà beneficiare della collaborazione con il Dipartimento di Information Systems dell'Università di Agder in Norvegia, dove è in corso una collaborazione focalizzata sulle tematiche di cybersecurity e IA.
Durata del periodo all'estero	4 mesi
Referente scientifico	Prof. Paolo Spagnoletti